Ministry of Electronics & IT

Government’s initiatives to strengthen security of cyber ecosystem, including against ransomware and Cross-Border Cybercrime

Posted On: 17 DEC 2025 12:51PM by PIB Delhi

The policies of the Government of India aim to ensure a safe, trusted, and accountable cyberspace. It remains vigilant and fully conscious of the cyber threat to India’s digital infrastructure.

Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) work continuously to safeguard digital services, including the critical sectors.

These agencies regularly monitor incidents, support timely response and ensure restoration. They conduct security and vulnerability audits under the Information Technology Act and Rules made under.

In this regard, CERT-In has developed and issued a Comprehensive Cyber Security Audit Policy Guidelines in July 2025 to carry out cyber security audits. These audits are done in a consistent, effective, and secure manner across sectors including critical infrastructure.

As per the guidelines, cyber security audit are conducted at least once in a year. It has empanelled 231 security auditing organizations to support and audit implementation of Information Security Best Practices.

In addition, the Government has undertaken several measures to strengthen security of cyber ecosystem including against ransomware and Cross-Border Cybercrime:

1. CERT-In is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.
2. It issues alerts & advisories regarding latest cyber threats/vulnerabilities including malicious attacks using AI and countermeasures regularly.
3. It advises remedial measures to affected organisations and coordinates incident response measures.
4. National Informatics Centre (NIC) carries out comprehensive security audit annually for its Critical Infrastructure to address the increasing number of ransomware attacks through CERT-In empanelled agencies including:

a) Information and Communication Technology infrastructure Audit of Central Ministries/Departments, States /UTs and National Data Centres.

b) Comprehensive Security Audit of Critical Web applications /databases/platforms.

c) Deployment of Unified Endpoint Management, Endpoint Detection and Response solutions across central ministries and departments for endpoint protection.

d) Removal of obsolete and legacy systems from the network.24×7 monitoring, detection, and mitigation of cyber threats using AI/ML and advanced security tools.

e) Continuous vulnerability assessments, system hardening, and proactive identification of application/system weaknesses.

f) Implementation of Zero Trust Security across NIC's ICT infrastructure.

g) Regular cybersecurity awareness programs for government employees.

5. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.
6. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of various organisations.
7. Establishment of sector-specific Computer Security Incident Response Teams (CSIRTs), such as CSIRT-Fin (Finance) and CSIRT-Power, to monitor & respond to cyber incidents within respective sectors.
8. Formulation of the Cyber Crisis Management Plan (CCMP) for all Government bodies to counter cyber-attacks and enable coordinated recovery.
9. 213 CCMP sensitisation workshops have been conducted to strengthen preparedness across organisations.
10. Development of indigenous cybersecurity tools by Centre for Development of Advanced Computing to reduce dependence on foreign solutions.

Expanding Cybersecurity Talent Pool

- Information Security Education & Awareness ("ISEA") program has been launched to generate awareness among users while using internet.
  - A dedicated website has been created for information security awareness that generates and upgrades relevant awareness material on a regular basis and can be accessed at https://www.infosecawareness.in.
- Certified Security Professional in Artificial Intelligence (CSPAI) program launched by CERT-In in September 2024 equips cybersecurity professionals with the skills to secure AI systems.
  - It helps in addressing AI-related threats, and ultimately ensure trustworthy AI deployment in business environments.

Cyber Swachhta Kendra (CSK)

It is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space

- It is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same
- It also provides cyber security tips and best practices for citizens and organisations
- Alerts regarding botnet/malware infections and vulnerable services are sent on a daily basis to organizations across sectors along with remedial measures.

This information was submitted by Union Minister of State for Electronics and Information Technology Shri Jitin Prasada in Lok Sabha on 17.12.2025.

***

MSZ

(Release ID: 2205047) Visitor Counter : 361

Read this release in: Marathi , हिन्दी , Tamil